Consultative Document / Document de consultation

Atomic Energy Control Board / Commission de contrôle de l'énergie atomique

CONSULTATIVE DOCUMENT C-98

Proposed Regulatory Policy Statement

REQUIREMENTS FOR RELIABILITY ANALYSIS OF SAFETY-RELATED SYSTEMS IN NUCLEAR REACTORS

Issued for comment:

April 14, 1987

Canada

This Consultative Document is issued in order to provide an opportunity for public review of the proposal it contains before formal issue as a Regulatory Document. Comments are encouraged and should be directed to the address below before JULY 14, 1987.

Subject to the Access to Information Act, all comments will be disclosed to the public and will be placed in the AECB Public Documents Room in the AECB offices at 270 Albert Street, Ottawa. Commentators should identify those parts of their comments that should not be disclosed pursuant to the Access to Information Act, the reason why they should not be disclosed, and also identify those parts that they consent to the disclosure of.

Direct comments to:

Health Effects and Regulatory
Documents Section
Atomic Energy Control Board
P.O. Box 1046
Ottawa, Ontario
CANADA
K1P 5S9

THE AECB REGULATORY DOCUMENTS SYSTEM

1. Siting, design, manufacture, construction, commissioning, operation, and decommissioning of nuclear facilities, or the production, possession, use and disposal of prescribed substances, in Canada or under Canadian control, are subject to the provisions of the Atomic Energy Control Act and Regulations administered by the Atomic Energy Control Board (AECB).

2. In addition to the Atomic Energy Control Regulations, three other categories of Regulatory Document are employed by the AECB. These are:

   Generic Licence Conditions - standard sets of conditions that are included in particular AECB licences of a common type, unless specific circumstances indicate otherwise;

   Regulatory Policy Statements - firm expressions that particular "requirements" not expressed as Regulations or Licence Conditions be complied with or that any requirements be met in a particular manner but where the AECB retains the discretion to allow deviations or to consider alternative means of attaining the same objectives where a satisfactory case is made; and

   Regulatory Guides - guidance or advice on any aspect of the AECB's regulatory process that is given in a manner less rigid than that intended by Policy Statements.

3. In developing Regulatory Documents, the AECB publishes its proposals as Consultative Documents in order to solicit comments both from the nuclear industry and from the public. This is done prior to releasing any Regulatory Document in final form. In certain cases, after the period for public comment, a Consultative Document may be issued for "trial use". This is done for a limited period of time to gain practical experience. Following the period of trial use, the revised document is re-issued for further public comment prior to release in final form.

4. Comments on Consultative Documents and suggestions for new Regulatory Documents and for improvement to those that exist are encouraged and should be directed to the Health Effects and Regulatory Documents Section of the AECB.

5. Copies of Consultative Documents, Regulatory Documents and related index lists are available in both English and French on request from the Office of Public Information. Requests for technical information on and interpretation of documents should be addressed to this office.

6. The Atomic Energy Control Board may be contacted as follows:

   Postal address: Atomic Energy Control Board
   P.O. Box 1046
   Ottawa, Ontario
   CANADA
   K1P 5S9

   Telephone
   General Inquiries: (613) 995-5894

TABLE OF CONTENTS

		PAGE
1.	INTRODUCTION AND SCOPE	1
2.	GENERAL REQUIREMENTS	1
3.	DEFINITION OF SYSTEM FAILURES	2
4.	DOCUMENTATION	2
5.	RELIABILITY DATA	3

REQUIREMENTS FOR RELIABILITY ANALYSIS OF SAFETY-RELATED SYSTEMS IN NUCLEAR REACTORS

1. INTRODUCTION AND SCOPE

1.1 This document defines general principles for reliability analyses of safety-related systems in nuclear reactors.

1.2 This document should be used whenever a reliability analysis is carried out to support an application for approval of construction or for renewal of a licence or to fulfill a licensing requirement.

1.3 It is the responsibility of the applicant when applying for approval of construction to define to the satisfaction of the Atomic Energy Control Board how the reliability analysis will be used in the design and safety assessment of the facility. The information that shall be provided includes:

(a) the organization and interaction of the various groups involved in the design, operation, and reliability analysis;

(b) the systems which will be analyzed and their design reliability requirements;

(c) the reliability analysis techniques which will be used and a justification of their adequacy.

2. GENERAL REQUIREMENTS

2.1 Any reliability analysis performed to satisfy licensing requirements should be part of a process which starts at an early design stage and continues appropriately throughout the operating life of the analyzed system.

2.2 Reliability analyses shall be consistent with the detailed design requirements of the analyzed system, and shall address all permissible modes of operation of the system.

2.3 Boundaries between systems or subsystems shall be clearly and unambiguously defined. Reliability analyses of connected systems or subsystems shall be fully compatible and consistent with each other.

2.4 Reliability analyses shall be consistent with the approved plant design and with the operating procedures in accordance with information available at the date stated in the reliability analysis report.

2.5 A procedure shall be established for determining the changes between the information used in the analysis and the current status. This procedure should address:

(a) design changes anticipated but not implemented;

(b) design changes made subsequent to the analysis;

(c) differences between actual operating or maintenance procedures and the procedure assumed in the analysis;

(d) differences in actual component and system performances from those assumed in the analysis.

3. DEFINITION OF SYSTEM FAILURES

3.1 Each reliability analysis report shall clearly define what constitutes failure of the analyzed system, including failures of its components and supporting equipment. The defined system failure shall be related to the overall safety assessment of the facility (in the Safety Report or other documents submitted in support of the licence application).

3.2 The definition of system failures of special safety systems or safety-related systems should include the following.

(a) The system or equipment fails to function as required. This includes both the inability to function at the time of request, and a loss of ability to function during a period in which the function is, or may be, required.

(b) The system or equipment does not cease to function on command (if applicable).

(c) The system or equipment starts functioning spuriously (if applicable).

3.3 Where possible, failure criteria should be stated in units that can be verified in practice by inspection or testing.

3.4 The reliability analysis should provide a comprehensive coverage of all factors which could cause system failures, without a priori assumptions that certain factors can be excluded.

3.5 The reliability analysis should also identify any failures of components of the analyzed system which could have safety implications for systems or equipment other than the system being analyzed.

4. DOCUMENTATION

4.1 Each reliability analysis performed to satisfy licensing requirements shall be documented with sufficient clarity that it can be readily and reliably used and audited by personnel other than the analysts.

4.2 A reliability analysis used in the licensing process shall be documented in such a way that it can be verified as far as practicable by test and observation during the complete life of the analyzed system, and in such a way that it can be maintained in an up-to-date state if design or operational changes are made to the system, its components, or supporting equipment, or if reliability data for any components or systems require modification.

4.3 Each event or other factor in a reliability analysis shall be identified in accordance with a defined scheme. Such a scheme should provide for the assignment of a unique identification to each different event or factor. If the same event or factor occurs more than once in the analysis, it should be assigned the same identification. The scheme should make it possible to relate each event to the specific component or components to which it refers.

5. RELIABILITY DATA

Data used in a reliability analysis shall be demonstrably valid.

Consultative Document / Document de consultation

Atomic Energy Control Board / Commission de contrôle de l'énergie atomique

DOCUMENT DE CONSULTATION C-98

Projet de déclaration de principe en matière de réglementation

EXIGENCES CONCERNANT L'ANALYSE DE FIABILITÉ DES SYSTÈMES LIÉS À LA SÛRETÉ DANS LES RÉACTEURS NUCLÉAIRES

Publié pour commentaires :

le 14 avril 1987

Canada

Le présent document de consultation est publié dans le but de fournir au public l'occasion d'examiner le projet qu'il contient avant qu'il soit adopté dans sa forme définitive comme document de réglementation. Le public est invité à faire parvenir ses observations à l'adresse indiquée ci-dessous avant le 14 JUILLET 1987.

Sous réserve de la Loi sur l'accès à l'information, toutes les observations seront communiquées au public et déposées dans la Salle des documents publics au siège social de la CCEA, au 270, rue Albert, Ottawa. Ceux et celles qui font des observations sont priés d'indiquer clairement quelles parties de leurs commentaires ne devraient pas être communiquées au public en vertu de la Loi sur l'accès à l'information et justifier leur demande; ils devraient, d'autre part, indiquer quelles parties ils autorisent à communiquer au public.

Veuillez adresser vos commentaires à l'adresse suivante :

Section des effets sur la santé et
des documents de réglementation
Commission de contrôle de l'énergie atomique
C.P. 1046
Ottawa (Ontario)
CANADA
K1P 5S9

TEXTES DE RÉGLEMENTATION DE LA CCEA

1. Le choix d'emplacement, la conception, la fabrication, la construction, la mise en service, l'exploitation et le déclassement d'installations nucléaires ou la production, la possession, l'utilisation et l'élimination de substances prescrites, au Canada ou sous contrôle canadien, sont assujettis aux dispositions de la Loi sur le contrôle de l'énergie atomique et de son Règlement d'application, dont l'administration relève de la Commission de contrôle de l'énergie atomique (CCEA).

2. En plus du Règlement susmentionné, la CCEA utilise trois catégories de textes de réglementation. En voici une courte description.

   Conditions générales d'autorisation de permis - ensemble de conditions types figurant dans tous les permis similaires délivrés par la CCEA, à moins de circonstances exceptionnelles;

   Déclarations de principe en matière de réglementation - déclarations laissant clairement entendre que certaines "exigences" qui ne figurent ni dans le Règlement ni dans les conditions des permis sont obligatoires ou que certaines exigences doivent être respectées d'une façon déterminée laissant également entendre que la CCEA se réserve le droit de permettre des écarts ou d'envisager d'autres façons d'en arriver aux mêmes fins, lorsque ces façons semblent convenir; et

   Guides de réglementation - directives ou conseils donnés sur tout aspect de la réglementation assurée par la CCEA mais formulés de façon moins rigoureuse que dans les déclarations de principe.

3. Lors de l'élaboration de ses textes de réglementation, la CCEA en publie d'abord le projet à titre de Document de consultation, afin de connaître les commentaires du secteur nucléaire et du grand public, avant que le projet de texte de réglementation paraisse sous sa forme définitive. Dans certains cas, après l'achèvement de la période réservée aux commentaires, la Commission peut faire mettre le document de consultation à l'essai pratique pour un temps limité. Après cette période d'essai, on demande encore une fois l'opinion du public, avant que le document révisé soit publié sous sa forme définitive.

4. Tout commentaire sur les documents de consultation et toute suggestion à l'égard des nouveaux textes de réglementation ou ceux déjà en vigueur sont les bienvenus; il suffit de les transmettre à la section des Effets sur la santé et documents de réglementation de la CCEA.

5. On peut se procurer des exemplaires des documents de consultation et des textes de réglementation, dans les deux langues officielles, en s'adressant au Bureau d'information publique. Toute demande de renseignements techniques ou d'interprétation des textes devrait être acheminée au Bureau susmentionné.

6. L'adresse de la CCEA est la suivante:

   Commission de contrôle de l'énergie atomique
   C.P. 1046
   Succursale "B"
   OTTAWA (Ontario)
   CANADA K1P 5S9

   Renseignements: (613) 995-5894

TABLE DES MATIÈRES

1. INTRODUCTION ET PORTÉE 1

2. EXIGENCES GÉNÉRALES 1

3. DÉFINITION DES DÉFAILLANCES DES SYSTÈMES 2

4. DOCUMENTATION 2

5. DONNÉES SUR LA FIABILITÉ 3

EXIGENCES CONCERNANT L'ANALYSE DE FIABILITÉ DES SYSTÈMES LIÉS À LA SÛRETÉ DANS LES RÉACTEURS NUCLÉAIRES

1. INTRODUCTION ET PORTÉE

1.1 Le présent document établit les principes généraux des analyses de fiabilité pour les systèmes liés à la sûreté dans les réacteurs nucléaires.

1.2 Le présent document devrait être utilisé chaque fois qu'une analyse de fiabilité est effectuée pour appuyer une demande de permis de construction ou de renouvellement de permis, ou pour satisfaire une exigence du permis.

1.3 Il incombe à la personne qui demande un permis de construction de déterminer à la satisfaction de la Commission de contrôle de l'énergie atomique de quelle manière l'analyse de fiabilité sera utilisée dans l'évaluation de la conception et de la sûreté de l'installation. L'information à fournir comprend :

a) l'organisation et l'interaction des divers groupes qui participent à l'analyse de la conception, de l'exploitation et de la fiabilité;

b) les systèmes à analyser et les exigences de fiabilité de leur conception;

c) les techniques d'analyse de fiabilité à utiliser et leur pertinence.

2. EXIGENCES GÉNÉRALES

2.1 Toute analyse de fiabilité effectuée pour satisfaire les exigences du régime de permis devrait faire partie d'un processus qui débute assez tôt au cours du stade de la conception et se poursuivre, comme il convient, tout au long de la vie utile du système analysé.

2.2 Les analyses de fiabilité doivent correspondre aux exigences détaillées de la conception du système analysé et doivent porter sur tous les modes d'exploitation autorisés du système.

2.3 Les limites entre les systèmes et les sous-systèmes doivent être déterminées clairement et sans ambiguïté. Les analyses de fiabilité des systèmes ou sous-systèmes reliés doivent être entièrement compatibles et cohérentes entre elles.

2.4 Les analyses de fiabilité doivent correspondre à la conception approuvée de la centrale et aux méthodes d'exploitation, conformément à l'information disponible à la date indiquée dans le rapport d'analyse de fiabilité.

2.5 Une méthode doit être établie pour déterminer s'il y a des différences entre l'information utilisée dans l'analyse et la situation actuelle. Cette méthode devrait traiter :

a) les changements de conception prévus, mais non mis en oeuvre;

b) les changements de conception apportés après l'analyse;

c) les différences entre les méthodes d'exploitation ou de maintenance actuelles et les méthodes supposées dans l'analyse;

d) les différences entre le rendement réel des composants et des systèmes et le rendement supposé dans l'analyse.

3. DÉFINITION DES DÉFAILLANCES DES SYSTÈMES

3.1 Tout rapport d'analyse de fiabilité doit indiquer clairement ce qui constitue une défaillance du système analysé, y compris les défaillances de ses composants et de son équipement d'appui. Il faut établir le rapport entre la défaillance indiquée du système et l'ensemble de l'évaluation de sûreté de l'installation (dans le rapport de sûreté ou tout autre document soumis à l'appui de la demande de permis).

3.2 L'indication des défaillances des systèmes spéciaux de sûreté ou des systèmes liés à la sûreté devrait inclure ce qui suit :

a) le système ou l'équipement ne fonctionne pas comme prévu. Cette défaillance comprend aussi bien l'incapacité de fonctionner au moment de la demande, de même que la perte de capacité de fonctionner durant une période où le fonctionnement est ou peut être requis;

b) le système ou l'équipement ne cesse pas de fonctionner sur commande (selon le cas);

c) le système ou l'équipement se met en marche par inadvertance (selon le cas).

3.3 Les critères de défaillance devraient être indiqués, si possible, en unités vérifiables en pratique, soit par des inspections soit par des essais.

3.4 L'analyse de fiabilité devrait couvrir la totalité des facteurs qui peuvent causer des défaillances de système, sans supposer a priori que certains facteurs peuvent être exclus.

3.5 L'analyse de fiabilité devrait déterminer aussi toutes les défaillances des composants du système analysé qui peuvent avoir des incidences en matière de sûreté sur des systèmes ou de l'équipement autres que le système analysé.

4. DOCUMENTATION

4.1 Toute analyse de fiabilité effectuée afin de satisfaire les exigences du permis doit être accompagnée de documents suffisamment clairs pour qu'elle puisse être utilisée de manière rapide et fiable et être vérifiée par des employés autres que les analystes.

4.2 Toute analyse de fiabilité utilisée dans le cadre du régime de permis doit être documentée de telle manière qu'elle puisse, dans la mesure du possible, être vérifiée par des essais et des observations tout au long de de la vie utile du système analysé, et de telle manière qu'elle puisse être mise à jour si des changements de conception ou de fonctionnement sont apportés au système, à ses composants ou à son équipement d'appui, ou encore s'il faut modifier les données sur la fiabilité de tout composant ou système.

4.3 Chaque événement ou autre facteur d'une analyse de fiabilité doit être désigné conformément à un plan déterminé qui devrait comporter une désignation unique pour chaque événement ou facteur. Si le même événement ou facteur revient plus d'une fois dans l'analyse, il devrait avoir la même désignation. Selon ce plan, il devrait être possible d'établir une relation entre chaque événement et le ou les composants particuliers auxquels il se rapporte.

5. DONNÉES SUR LA FIABILITÉ

La validité des données utilisées dans les analyses de fiabilité doit être démontrable.